

**Annual 47 C.F.R. § 64.2009(e) CPNI Certification**

Annual 64.2009(e) CPNI Certification for 2019 covering the prior calendar year 2018

1. Date filed: February 19, 2019
2. Name of company covered by this certification: JumpFiber, LLC
3. Form 499 Filer ID: 832237
4. Name of signatory: Corky Roth
5. Title of signatory: Chief Executive Officer
6. Certification:

I, Corky Roth, certify that I am Chief Executive Officer of JumpFiber, LLC ("Company") and, acting as an agent of the Company, that I have personal knowledge that the Company has established operating procedures, summarized in the attached statement, that are adequate to ensure compliance with the customer proprietary network information ("CPNI") rules as set forth in Part 64, Subpart U of the Commission's rules, 47 C.F.R. §§ 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the Company's procedures ensure that the Company is in compliance with the requirements set forth in Section 64.2001 *et seq.* of the Commission's rules (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review).

The Company has not received any customer complaints in the past calendar year concerning the unauthorized release of CPNI, and is not aware of any unauthorized disclosures of CPNI. Company has not taken any actions against data brokers, including proceedings instituted or petitions filed by the company at either state commissions, the court system or at the Commission.

I hereby represent and warrant that the above certification is consistent with Section 1.17 of the Commission's rules, 47 C.F.R. § 1.17, which requires truthful and accurate statements to the Commission, and acknowledge that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject the Company to enforcement actions.



Corky Roth  
Chief Executive Officer  
JumpFiber, LLC

Executed February 16th, 2019

## **CPNI Compliance Policies of JumpFiber, LLC**

The following summary describes the policies of JumpFiber, LLC (“JumpFiber”) that are designed to protect the confidentiality of Customer Proprietary Network Information (“CPNI”) and to assure compliance with the rules of the Federal Communications Commission (“FCC”) set forth in 47 C.F.R. Part 64, Subpart U, Section 2001 *et seq.* CPNI is “(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.”

These policies are managed by JumpFiber’s CPNI Compliance Manager, Ron Clark.

### **I. USE, DISCLOSURE OF, AND ACCESS TO CPNI**

JumpFiber will use, disclose, or permit access to individually identifiable CPNI only in its provision of the communications service from which such information is derived; for services necessary to, or used in, the provision of such communications service, including the publishing of directories; to initiate, render, bill and collect for communications services; to protect the rights or property of JumpFiber, or to protect users or other carriers or service providers from fraudulent, abusive or unlawful use of, or subscription to, such services; to provide inside wiring installation, maintenance, or repair services; as required by law; or as expressly authorized by the customer.

JumpFiber does not use CPNI to market service offerings among the different categories of service, or even within the same category of service, that it provides to subscribers. Although JumpFiber’s current policy is not to use CPNI for marketing, in the event that any employee or agent wishes to use CPNI for marketing or to seek customer approval for such use, such proposed use is subject to a supervisory review process that shall involve the CPNI Compliance Manager. If such use is approved, JumpFiber shall modify these policies and conduct additional training as needed to assure compliance with the FCC’s rules.

JumpFiber does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

When JumpFiber receives or obtains proprietary information from another carrier for purposes of providing a telecommunications service, it shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

### **II. SAFEGUARDS AGAINST DISCLOSURE OF CPNI TO UNAUTHORIZED PARTIES**

Above and beyond the specific FCC requirements, JumpFiber will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. If any employee becomes aware of new methods that are being used or could be used by third parties to attempt to obtain unauthorized access to CPNI, or of possible changes to JumpFiber’s existing policies

that would strengthen protection of CPNI, they should report such information immediately to the CPNI Compliance Manager so that JumpFiber may evaluate whether existing policies should be supplemented or changed.

**A. Inbound Calls to JumpFiber Requesting CPNI**

JumpFiber does not disclose any CPNI to an inbound caller until the caller's identity has been authenticated.

More stringent protections apply to Call Detail Information (CDI), which includes any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call. Even after a caller has been authenticated under the process above, JumpFiber does not reveal CDI to an inbound caller. Instead, if an inbound caller requests CDI, JumpFiber may offer to provide the requested CDI by sending the information by mail to a mailing address of record for the account, but only if such address has been on file with JumpFiber for at least 30 days, or by calling back the customer at their telephone number of record.

**B. Online Access to CPNI**

At this time, JumpFiber does not provide online access to CPNI. In the event that it offers such access in the future, it will implement authentication methods that are consistent with FCC rules.

**C. In-Person Disclosure of CPNI**

JumpFiber does not routinely make CPNI available at its offices. However, in the event that a customer requests CPNI in person, JumpFiber may disclose a customer's CPNI to an authorized person only upon verifying that person's identity through a valid, non-expired government-issued photo ID (such as a driver's license, passport, or comparable ID) matching the customer's account information.

**D. Notice of Account Changes**

Whenever a Customer's address of record is created or changed, JumpFiber will send a notice to customer's prior address of record notifying them of the change. These notifications are not required when the customer initiates service. The notice provided under this paragraph will not reveal the changed information and will direct the customer to notify JumpFiber if they did not authorize the change.

**E. Business Customer Exemption**

The authentication requirements for disclosure of CPNI do not apply to disclosure of business customer information by a dedicated account representative who knows through personal experience that the person requesting the information is authorized representative of the customer and that the contract between JumpFiber and that business customer specifically addresses the protection of the customer's CPNI.

### **III. REPORTING CPNI BREACHES TO LAW ENFORCEMENT**

Any JumpFiber employee that becomes aware of any breaches, suspected breaches or attempted breaches must report such information immediately to the CPNI Compliance Manager. Such information must not be reported or disclosed by any employee to any non-employee, including the potentially affected customer, except in express conformance with the procedures described below. Any employee that fails to report such information will be subject to disciplinary action that may include termination.

It is JumpFiber's policy that employees should not be discouraged from reporting information about breaches that may have been caused in part by their own actions or omissions. Once a breach has occurred, the most important objective is to attempt to limit the damage to our customers, make any adjustments as needed to prevent a recurrence of the breach, and to alert law enforcement promptly. Therefore, although employees who violate JumpFiber's CPNI compliance procedures are subject to discipline, the sanctions may be substantially reduced where employees promptly self-report violations if appropriate.

#### **A. Identifying a "Breach"**

A "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI. If an employee has information about an incident and is not certain that the incident would not constitute a breach under this definition, the incident must be reported to the CPNI Compliance Manager.

If a JumpFiber employee determines that an unauthorized person is attempting to gain access to CPNI but does not succeed at doing so, no breach has occurred. However, the incident must be reported to JumpFiber's CPNI Compliance Manager who will determine whether to report the incident to law enforcement and/or take other appropriate action. The CPNI Compliance Manager will determine whether it is appropriate to update JumpFiber's CPNI policies or training materials in light of any new information; the FCC's rules require JumpFiber on an ongoing basis to "take reasonable measures to discover and protect against activity that is indicative of pretexting."

#### **B. Notification Procedures**

As soon as practicable, and in no event later than seven (7) business days upon learning of a breach, the CPNI Compliance Manager shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) by accessing the following link: <https://www.cpnireporting.gov>. JumpFiber will not notify customers or disclose a breach to the public until 7 full business days have passed after notification to the USSS and the FBI, and will defer such notification at the request of either agency. If JumpFiber receives no response from law enforcement after the 7<sup>th</sup> full business day, it must promptly proceed to inform the customers whose CPNI was disclosed of the breach.

### **IV. RECORD RETENTION**

The CPNI Compliance Manager is responsible for assuring that we maintain for at least two years a record, electronically or in some other manner, of any breaches discovered,

notifications made to the USSS and the FBI pursuant to these procedures, and notifications of breaches made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

JumpFiber maintains a record, for a period of at least one year, of those limited circumstances in which CPNI is disclosed or provided to third parties or where third parties were allowed access to CPNI. If JumpFiber later changes its policies to permit the use of CPNI for marketing, it will revise its recordkeeping policies to comply with the Commission's recordkeeping requirements.

JumpFiber maintains a record of all customer complaints related to their handling of CPNI, and records of JumpFiber's handling of such complaints, for at least two years. The CPNI Compliance Manager will assure that all complaints are reviewed and that JumpFiber considers any necessary changes to its policies or practices to address the concerns raised by such complaints.

JumpFiber will have an authorized officer, as an agent of JumpFiber, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that JumpFiber has established operating procedures that are adequate to ensure its compliance with FCC's CPNI rules. The certificate for each year will be filed with the FCC by the first business day or on after March 1 of the subsequent year, and will be accompanied by a summary or copy of this policy that explains how JumpFiber's operating procedures ensure that it is in compliance with the FCC's CPNI rules. In addition, the filing must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI.

## **V. TRAINING**

All employees with access to CPNI receive training on JumpFiber's CPNI policies and are informed that (i) any use or disclosure of CPNI or other act or omission not in compliance with such policies will result in disciplinary action, including the termination of employment where appropriate, and (ii) employees who knowingly facilitate the unauthorized disclosure of a customer's confidential information may be subject to criminal penalties.